

Robotics Research for Cybersecurity

Wei-Min Shen

Polymorphic Robotics Laboratory

USC/ISI, 4676 Admiralty Way, Marina del Rey, CA 90292

Phone: 310-448-8710, Fax: 310-822-0751

Email: shen@isi.edu, Web: <http://www.isi.edu/robots/>

Executive Summary

This project is to conduct a comprehensive study of robotics research in the context of cybersecurity. Specifically, 1) Create a realistic cybersecurity test scenario which captures the unique and increasingly difficult robotics research challenges; 2) Survey the state-of-the-art in applicable research and technology; 3) Identify and analyze the salient research challenges with a primary focus on computational sciences. Define multiple dimensions of these challenges including relative difficulty as well as what is needed for robust autonomy; 4) Conduct a workshop with the goal of bringing together a multidisciplinary group of top researchers and also experts in cybersecurity to develop detail and prioritize research challenges for the next three to five years.

A Challenge Scenario

Cybersecurity demands many new capabilities that are beyond the current robotics technologies. Imagine, for example, that one must physically deliver a cyber-payload to a target location that is dangerous to access. A novel approach would be for some small robots to be delivered via smart munition to the vicinity of the target building. They must be *robust* to land safely and *intelligent* to find an entrance, enter the building, locate a computer in an office environment, and plug into a USB port. They must be *stealthy* to avoid detection, *agile* to overcome difficult terrain/obstacles, *collaborative* to leverage capabilities, *dexterous* to manipulate objects, *adaptive* to deal with unexpected damage or situations, and even *reconfigurable* to be physically joined together for new capabilities. Ultimately, they must be general and reusable for similar missions in different environments.

Studies Performed

1. Robotic scenario: We have created a comprehensive scenario and implemented in a physical experiment site for the scenario. The goal of this scenario is for a robot to enter a room via challenging entrance and delivery a small package into a slot similar to USB port. The entrance is a pipe system about 20 feet long and 10cm in diameter. It has a set of different difficult levels. The pipes can be straight, curved, disconnected, and have both 2D and 3D turns. In the 3D setting, there is a section that the robot must climb about 1 meter high in order to complete the entry. Once entered the room, the robot must climb on the top of an office desk and deliver a small package (USB size) into a slit that is similar to a USB port.
2. Organized a Robotics Challenge Competition at the 2011 International Conference for Robotics and Automation. Figure 1 shows some pictures taken

Report Documentation Page			Form Approved OMB No. 0704-0188		
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 25 JAN 2012		2. REPORT TYPE Final		3. DATES COVERED 07-09-2010 to 07-09-2011	
4. TITLE AND SUBTITLE Robotics Research for Cybersecurity			5a. CONTRACT NUMBER FA23861014156		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S) Wei-min Shen			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) University of Southern California, 4676 Admiralty Way, Suite 1001, Marina del Rey, CA, 90292-7008			8. PERFORMING ORGANIZATION REPORT NUMBER N/A		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) AOARD, UNIT 45002, APO, AP, 96338-5002			10. SPONSOR/MONITOR'S ACRONYM(S) AOARD		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S) AOARD-104156		
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT Studies performed are 1) Robotic scenario, 2) Robotics Challenge Competition at ICRA2011, 3) High-level survey of applicable technologies, and 4) Identification and discussion of the robotic challenges that must be sloved for cyber-security. The robotics community that is relevant to cyber-security has begun to realize the challenges faced by these tasks and formalize these challenges into feasible research programs that AFOSR might be interested in investigation.					
15. SUBJECT TERMS Cybersecurity, Cybersecurity, Robotics, Artificial Intelligence, Autonomous Agents and Multi-Agent Systems					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 3	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

from that competition. Two international teams and many robotics experts have participated and observed/commented the competition. More information can be found at the “Robotic Challenges” website at <http://www.icra2011.org>.

3. Perform a high-level survey of applicable technologies. Specifically, the results will be published as a chapter in the book titled “Collective Intelligence” to be published by Springer in 2012.
4. Identify and discuss the robotic challenges that must be solved for Cyber-Security. We anticipate some breakthroughs in the area of self-reconfigurable and modular robots for this particular challenge task within 3 to 5 years. There are several possible dimensions along which future research programs can be systematically organized, including a) the degree of pre-knowledge of the mission, b) the level of integration of capabilities, c) the scope of tasks and environments, d) the degree of autonomy, e) the extent of unexpectedness, and f) other quantities related to robust intelligence. In the context of cybersecurity, autonomy and unexpectedness are critical. This is because the robots will be likely not to be in communication, or only irregularly so, with the “home”, and inevitably encounter both expected and unexpected tasks. The expected tasks may include finding the entrances of the building, going through monitored areas without being detected, exploring internal spaces, creating maps, searching for targets, and returning to the outside. The unexpected tasks may include unfamiliar obstacles, unforeseen damage, unusual objects, and unanticipated needs for new capabilities. For instance, a robot may find a passage that is too narrow for its body or too high for its reach; may accidentally damage its body parts; may encounter a vertical rope hanging from upstairs; and may need an extra long arm. Furthermore, the entrance of the target building may be located in an area that is inaccessible by land so that the robots must be air delivered in proximity. In all these cases, the robot must intelligent enough to assess the situation and physically capable of changing its shape, size, and functions dynamically.

Conclusions

In this short study, the robotics community that is relevant to cyber-security has begun to realize the challenges faced by these tasks and formalize these challenges into feasible research programs that AFOSR might be interested in investigation.



Figure 1: Pictures from the Robotics Challenge Events at ICRA 2011 Conference.